CYBER SECURITY INTERNSHIP REPORT AT SHADOWFOX

NAME:- Aniket Ramesh Chavan

BATCH :- july2025

MAIL ID :- chavananiket5222@gmail.com

TASK LEVEL :- Beginner

BEGINNER LEVEL TASK

1: - Find all the ports that are open on the website
http://testphp.vulnweb.com/

REPORT OF TASK LEVEL

Introduction :-

Cyber security is now spreading in all over internet due to security and risks on the internet . websites are vulnerable due to is structure , security and build up . so here following a Way to identifying the website in vulnerable or not using scaning the open ports using tools and some tricks.

Website :- testphp.vulnweb.com

1. Port scanning :-

In port scanning we are cheacking the port of the website which is opened or not
Because most of the websites compromised due to open ports . port are vulnerable and easy to access the websites.

Task 1

Find all the ports that are open on the website http://testphp.vulnweb.com/

- **Attack Name :-** Port Scanning
- **Severity :-** High and its score 7.0 – 8.9

❖ Steps to reproduce with screenshot

Step 1 :- ip address identification:-

In this technique I used nslookup tool for idetifiy the ip of the given wesite.
Ip address is unique protocol used for internet services . targeting the ip is our goal .

Command :- nslookup testphp.vulnweb.com

Step 2 :- port scanning :-

In port scanning we are cheacking the port of the website which is opened or not .

I used nmap tool to scan the ports are opned or not

Command :- nmap -p- testphp.vulnweb.com

Here is result of port scanning

Website :- testphp.vulnweb.com

Ip address :- 44.228.249.3

Namp command :- nmap -p- 44.228.249.3

Analysis :-

Port / protocol :- 80/tcp

State :- open

Service :- http

Version :- nginx 1.19.0

Port 80 / tcp host is active htttp services . this web server using nginx 1.19.0 version tho secure the site update and upgrade the site with reguraly security patches .

Step 3 :- port scanning fig :-

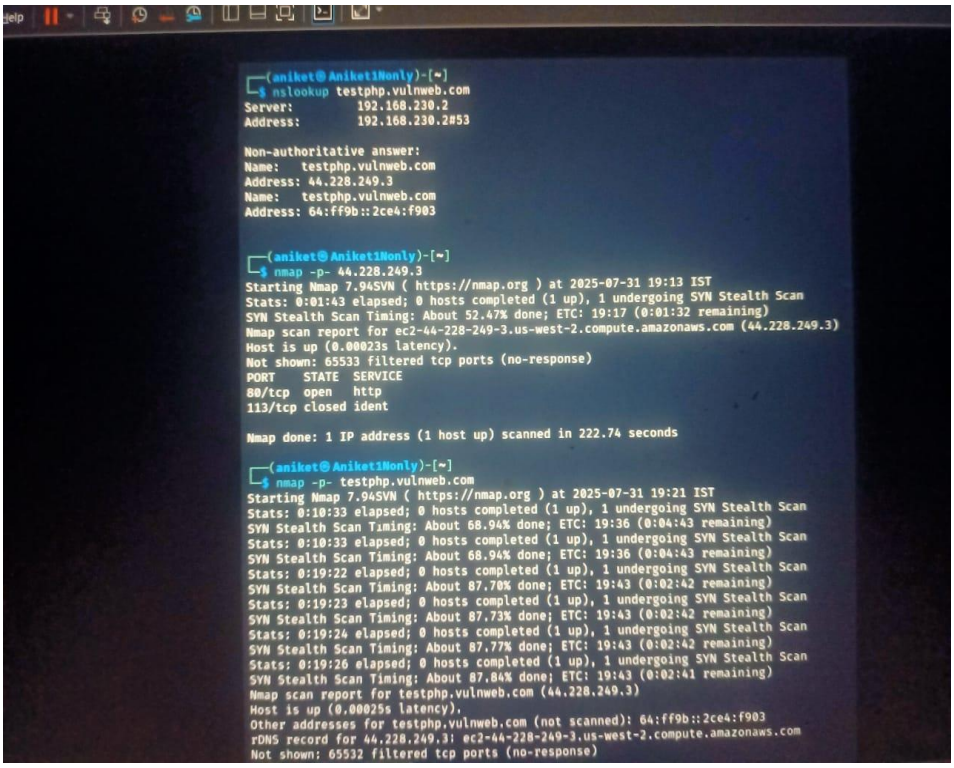

Fig :- nmap scanning

❖ Impact :-

Advantages :-

- Finds Websites or Web Services :-
  Port 80 is where most websites live. Scanning it helps you find if a website or web service is running.
- Not Very Suspicious :-
  port 80 is commonly used, scanning it doesn't usually raise red flags in firewalls or security systems.

Disadvantages :-

- Might Still Be NoticedWhile it's less obvious than other scans, if you scan too many times or too fast, you might still get caught.

- Limited Info

  Just knowing port 80 is open doesn't tell you much unless you look deeper into what's running on it.

❖ Mitigation steps :-

1. Block or limit access to port 80 from unknown or untrusted IPs. Only allow trusted users or networks to reach your web server.

2. Set Up Intrusion Detection/Prevention Systems (IDS/IPS)

Tools like Snort, Suricata, or cloud-based security services can detect and block scanning attempts.
They can alert you if someone is probing your port 80 repeatedly.

3. Always check the url and https or http protocol port 80
4. Set a limit acces to directories and authentications always check the system data is encrypted and safe
5. Update security patches and keep system updated .

❖ Resources used :-

Kali linux operating system , nmap tool (for scanning open ports), nslookup tool (for ip address identify)